THERE IS CLAIMED:

1. A method of providing access control for and/or vis-à-vis users who access a computer network enabling exchange of information, in particular the Internet, by means of terminals, via a private access node, shared or specific to an organization, such as a company, to which said terminals are connected to access said computer network via an access server, which method stores temporarily for downstream filtering the stream of multimedia data received from said computer network addressed to a user terminal in response to an access request formulated from said terminal, said downstream filtering being applied by an arrangement for authorizing or blocking transmission of said data stream to said terminal as a function of particular criteria applied to the received data stream at said private access node.
2. The method claimed in claim 1 wherein said data received from said computer network is stored temporarily before it is transmitted to said user terminal or not, depending on the results of an analysis.
3. The method claimed in claim 2 wherein data received from said computer network that is not transmitted, following an analysis that leads to a decision not to transmit it to said user, is retained so that said data can be compared with data of a subsequent data stream to accelerate decision-making in the case of identical data in different data streams, for a particular set of data, without having to carry out a further analysis corresponding to that which led to the data that is retained not being transmitted.
4. The method claimed in claim 1 wherein transfer of data received from said computer network to a user terminal is temporarily delayed in said temporary storage means pending determination of conformance of what has been received with particular standards and then transmitted to said terminal if conformance is found.
5. The method claimed in claim 4 wherein temporarily delayed data relating to a data stream stored in the conformance determination phase is retained to enable a further check in the event of non-conformance, either in respect of data received on detection of non-conformance, in which case the data stream that transmits it from said computer network is interrupted, or in respect of all of the data received, without said data stream being interrupted.
6. The method claimed in claim 4 wherein data for which and/or for the source of which non-conformance has been detected in a received data stream is retained

to enable interruption of a data stream subsequently received before complete analysis of the data that said data stream transmits if said data and/or said source are detected again in said stream subsequently received.

7. The method claimed in claim 1 including counting, for control purposes, a particular content, consisting of a characteristic combination of data, if said content is found in said temporarily stored data, after it has been received from said computer network in at least one data stream addressed to a particular terminal.

8. The method claimed in claim 2 including signature analysis for at least temporarily blocking transmission of data received from said network to a user terminal if said data incorporates a signature characteristic of restricted signaling rights.

9. The method claimed in claim 2 including an identifier search analysis applied to received data addressed to a user terminal to authorize transmission of said data to said terminal if one or more particular identifiers are found in the received data addressed to said terminal.

10. An arrangement for providing access control for and/or vis-à-vis users who access a computer network enabling exchange of information, in particular the Internet, from terminals via a private access node that is shared or specific to an organization, such as a company, and to which said terminals are connected to access a computer network via a service provider, which arrangement includes hardware means and/or software products organized to authorize or block transmission of said data stream to said terminals as a function of particular criteria applied to said received data stream at said private access node.